Consolidated Technology Services • WA

Service Issue
ActiveSync Mobile Messaging Service

September 2012

Overview

CTS implemented ActiveSync Mobile Messaging in April 2012. ActiveSync is integrated with Exchange 2010 and offers a less expensive alternative to BlackBerry Mobile Messaging. As implemented, CTS is responsible to test devices for compliance with the OCIO Security Standard. Only CTS approved devices are allowed. New devices are reviewed, tested, and updated quarterly.

Issues

There are two related issues:

1. Vendor (carrier) deployment of device OS upgrades

   In the last few weeks Verizon pushed a new operating system to a number of its Android customers. The OS upgrade changed the model id on the device. These devices immediately went into quarantine as ActiveSync uses the model id to allow access. The end result is the device that worked yesterday is not working today, and will not work until the device is retested and approved.

2. Turnaround for testing new or quarantined devices

   Device testing requires two things – an available device and time to test.

   Device availability – There are hundreds of potential devices in today's bring your own device (BYOD) world. It is not practical for CTS to have a standing inventory of all devices in use. Vendors release new devices multiple times per year. Testing a particular device is contingent upon access to either a carrier-provided or customer-provided device.

   Time to test - It takes several hours to completely test a device for compliance with the OCIO Security standard. There are approximately 19 required tests and some, due to the nature of the test, require a specific amount of wait time. For example, testing the 1 hour password timeout feature requires at least 1 hour.

Options

1. Maintain the status quo

CTS continues in the role of approving new and quarantined devices. Expectation of service delivery needs additional discussion and acceptance.

2. Allow-Push

   Allow all devices into ActiveSync. CTS pushes an OCIO compliant policy to the device upon activation. It is then incumbent on the agency to ensure policy compliance.

3. Distributed Testing

   In this option, CTS shares testing responsibility with customer agencies. A testing matrix is provided to customer agencies who then, following the testing matrix, determine if a device is compliant with the OCIO security standard. This has the potential to improve service delivery by shortening the time necessary to obtain a test device. Typically, the agency already has the device and can test immediately.

Questions for Discussion

What is a reasonable turnaround time for device testing?

Does an approved device need retesting following an OS upgrade?

Should CTS or the customer agency be in the role of ensuring OCIO Security Standard compliance for mobile devices?

Current testing practices add cost and delay. Are they necessary?